Express Mail Label No. EJ686572582US 12-20-99 A

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
JA9-98-173

Total Pages in this Submission
(30 excluding certified copy)

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

SYSTEM FOR AUTHENTICATING DIGITAL DATA

and invented by:

KOICHI KAMIJO; NORISHIGE MORIMOTO; TOHRU SAKAKURA; and AKIO KOIDE

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Which is a:

☐ **Continuation** ☐ **Divisional** ☐ **Continuation-in-part (CIP)** of prior application No.: _____

Enclosed are:

Application Elements

1. ☒ Filing fee as calculated and transmitted as described below
2. ☒ Specification having **15** pages and including the following:
   - a. ☒ Descriptive Title of the Invention
   - b. ☐ Cross References to Related Applications *(if applicable)*
   - c. ☐ Statement Regarding Federally-sponsored Research/Development *(if applicable)*
   - d. ☐ Reference to Microfiche Appendix *(if applicable)*
   - e. ☒ Background of the Invention
   - f. ☒ Brief Summary of the Invention
   - g. ☒ Brief Description of the Drawings *(if drawings filed)*
   - h. ☒ Detailed Description
   - i. ☒ Claim(s) as Classified Below
   - j. ☒ Abstract of the Disclosure

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
JA9-98-173

Total Pages in this Submission
(30 excluding certified copy)

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*

   a. ☒ Formal Number of Sheets 4

   b. ☐ Informal Number of Sheets _____

4. ☒ Oath or Declaration

   a. ☐ Newly executed *(original or copy)* ☒ Unexecuted

   b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*

   c. ☒ With Power of Attorney ☐ Without Power of Attorney

   d. ☐ *DELETION OF INVENTOR(S)*
   Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Computer Program in Microfiche *(Appendix)*

7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*

   a. ☐ Paper Copy

   b. ☐ Computer Readable Copy *(identical to computer copy)*

   c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers *(cover sheet & document(s))*

9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*

10. ☐ English Translation Document *(if applicable)*

11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations

12. ☐ Preliminary Amendment

13. ☒ Acknowledgment postcard

14. ☒ Certificate of Mailing

   ☐ First Class ☒ Express Mail *(Specify Label No.):* **EJ686572582US**

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
JA9-98-173

Total Pages in this Submission
(30 excluding certified copy

Accompanying Application Parts (Continued)

15. ☒ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*

16. ☐ Additional Enclosures *(please identify below):*

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	9	- 20 =	0	x $18.00	$0.00
Indep. Claims	1	- 3 =	0	x $78.00	$0.00
Multiple Dependent Claims (check if applicable) ☐					$0.00
				BASIC FEE	$760.00
OTHER FEE ***(specify purpose)*** _____					$0.00
				TOTAL FILING FEE	$760.00

☐ A check in the amount of to cover the filing fee is enclosed.

☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. **09-0463** as described below. A duplicate copy of this sheet is enclosed.

- ☒ Charge the amount of **$760.00** as filing fee.
- ☒ Credit any overpayment.
- ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Lawrence D. Cutter

Signature

Dated: **December 17, 1999**

Lawrence D. Cutter - Attorney
Registration No. 28,501
IBM Corporation
Intellectual Property Law
522 South Road, M/S P386
Poughkeepsie, NY 12601-5400
Telephone: (914) 433-1172
Facsimile: (914) 432-9601

cc:

Docket No : **JA9-98-173**

Inventor : **K. Kamijo et al**

Title : **System For Authenticating Digital Data**

APPLICATION FOR UNITED STATES

LETTERS PATENT

"Express Mail" Mailing Label No.: **EJ686572582US**
Date of Deposit: **December 17, 1999**

I hereby certify that this paper is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Box Patent Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Name: **Billy R. Stacy**

Signature: Billy R. Stacy

INTERNATIONAL BUSINESS MACHINES CORPORATION

Sheet 1 of 95

SYSTEM FOR AUTHENTICATING DIGITAL DATA

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a system for recording digital data for maintenance, namely prevention of tampering or changing of digital data transferred via memory for temporarily storing data from a digital data input device such as a digital camera, particularly to a system capable of preventing changes to a digital photograph for assessment of non-life insurance or for recording work on a building site taken by a digital camera.

Best Available Copy

2. Description of the Related Art

In recent years, digital data is increasingly used in a number of fields due to rapid proliferation of consumer digital devices such as a digital camera. However, digital data is accompanied by a risk to be used as evidence since there is a danger of contents being changed without leaving a trace. In order for a recipient of data to trust any data, there should be a means for assuring that the data has not been changed since it was acquired.

As a method to prevent tampering or changing of digital data, there are methods such as MAC (Message Authentication Coding) where an electronic signature created by a one-way hash function is transferred being attached to the data. In the case of a digital image, it is also possible to further enhance conformity of the electronic signature with an embedded image by using an electronic watermark in the image (for instance, Japanese Unexamined Patent Publication No. Hei 10-164549).

However, if application to a digital photograph which supposedly needs this technology most of all is considered, it will be inside a camera that an electronic signature is implemented. In that case, a more reliable system is desired since an encryption key stored in the camera is fixed in

addition to high load of computation on the camera. Namely, a method which is implementable within constraints of current hardware and capable of ensuring necessary and sufficient integrity of data has been required.

An object of the present invention is to resolve the above-mentioned problem and to provide a system for authenticating digital data capable of preventing change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data.

SUMMARY OF THE INVENTION

The present invention covers a system for writing digital data entered from an input device to a memory and transferring the digital data written in the memory to a receiving device. In this system, first of all, when writing digital data from the input device to the memory and transferring the digital data from the memory to the receiving device, devices are authenticated between the input device and the memory and between the memory and the receiving device respectively. At the same time, when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, the implemented electronic signature is decrypted so as to transfer the digital data after ensuring that it has not been changed since it was recorded.

In the present invention, first of all, when writing data from an input device for digital data to a memory and transferring the data from the memory to a receiving device, it is possible to authenticate the respective device so as to limit a data transfer route to the receiving device via the memory from the input device of digital data. It is also possible, when recording data in the memory, to prevent any change of data caused by a direct access to the memory by implementing on the data an electronic signature by a one-way hash function, preferably by a built-in central processing unit (CPU). This can prevent change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a drawing for describing an example of a system for authenticating digital data of the present invention.

Fig. 2 is a drawing showing the concept of authentication and data flow in the present invention.

Fig. 3 is a drawing showing an example of an internal structure of a CompactFlash memory card.

Fig. 4 is a drawing showing an example of a physical format of a CompactFlash memory card.

Fig. 5 is a drawing showing a page model in a CompactFlash memory card.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Fig. 1 is a drawing for describing an example of a system for authenticating digital data of the present invention. In the example shown in Fig. 1, input device 100 is a digital camera, memory 200 is a CompactFlash memory card, receiving device 300 is a personal computer for managing image data. Memory 200 is not limited to a detachable style and may be a memory built into a camera. Moreover, in the following description, "ordinary data transfer" means data transfer which operates properly even with an unspecified device without authentication. Furthermore, a digital camera with an authentication feature related to the present invention is referred to as SDC (Secured Digital Camera), a memory with an authentication feature related to the present invention as SCF (Secured CompactFlash), and a personal computer with an authentication feature related to the present invention as SPC (Secured Personal Computer). In addition, DC, CF and PC refer to a digital camera, a CompactFlash memory card, and a personal computer in general, respectively.

First, a prerequisite for implementing a system for authenticating digital data of the present invention is described. To begin with, specific and common commands (Request Seed and Send Seed commands) are defined among input device 100, memory 200 and receiving device 300 which are specified. While a general device returns an error to these commands, it results in time-out. Request Seed command is a command which requests the transmission of a seed to a client, and Send Seed command is a command which informs a client that a seed is to be transmitted. Next, between input device (SDC) 100 and memory (SCF) 200 which are specified, they have a specific encryption function Hdc and its key Kdc. Memory 200 also has a certain hash function Hcf and an internal key Kcf. They are stored in read-only memories (ROMs) of their respective devices and do not leak out of the devices. Even in case Hdc or Hcf leaks out, however, confidentiality is maintained.

Next, between memory (SCF) 200 and receiving device (SPC) 300 which are specified, they have a specific mutual encryption function Hpc and its key Kpc. In memory 200, Kpc is stored in NAND record space 210, encrypted by a certain encryption function Ex and its key Kx. Hpc, Ex and Kx are stored in a ROM of SCF. Also in receiving device 300, Kpc is encrypted by a certain encryption function E2pc and its key password. The password is either stored where an owner of SCF cannot access or itself encrypted. It is described in detail later. The functions of the devices in each process are described as follows, referring to Fig. 1.

1. Recording a digital image to memory

In Fig. 1, an image obtained at image capture section 110 is recorded in NAND record space 210 of memory 200 by way of image processing section 120. As for memory 200, when it receives a request for writing data from input device 100, authentication section 231 of memory 200 performs device authentication to authentication section 130 of input device 100 by way of built-in central processing unit (CPU) 220. If authentication is successful, an authentication flag is written when data recording is implemented from image processing section 120 to NAND record space 210. This authentication may also be configured to repeat intermittently even while data transfer continues so as to enhance a security level and so as not to have a

device replaced after success of device authentication. Its contents are described later. The following explains an actual process:

1.1. SDC transmits a Request Seed command to CF and requests a certain random number (= R1). In this case, if an error is returned or there is no response, SDC determines that CF is not SCF and performs ordinary data transfer.

1.2. SCF returns R1 to SDC. If an ordinary write command is received before a seed is requested, SCF determines that DC is not SDC and performs ordinary data transfer.

1.3. SDC starts data transfer. CF usually repeats data transfer of one page (= 512 bytes) 256 times at the maximum per write command.

1.4. If R1 is returned from CF in (1.2), SDC calculates by the following expression (1) R_Ed which is R1 encrypted by using a key Kdc and returns it to CF. Kdc is a secret key between SDC and SCF.

$$R_Ed = Hdc(Kdc, R1) \quad (1)$$

1.5. SCF calculates the above expression (1) by using Hdc and Kdc which it has and R1 which was sent to DC, so as to check if R_Ed matches what came from DC. If R_Ed does not match it, it is determined that DC is not SDC, and data transfer for the write command this time becomes an ordinary data transfer including that page.

2. Data protection in memory

If R_Ed matches in the above (1.5), SCF further attaches, before next authentication is performed, an authentication mark (flag) generated at the CPU to an image to be recorded to a receiving page and implements an electronic signature to record it in NAND record space 210. If there is no authentication, it records it without attaching any authentication mark. CF has a

redundant area of 16 bytes per page not to be calculated by ECC, and 4 bytes of the area is a reserved area in which the flag can be written. Detailed configuration of a CompactFlash memory card is described later. While an authentication mark is acquired by taking hash of the sent data, if it is costly to take hash for all of the data, data to be hashed may also be determined by cipher. In this case, although there should be concern about security because hash is not taken from the entire data, security is considered to be sufficiently maintained since data from DC is normally compressed by JPEG and changing data itself by swapping by the portion (1 byte for instance) is very difficult. Here, for calculation of hash, Kcf which is a unique key to each SCF built into a ROM of SCF is used. As long as Kcf is confidential, hash function Hcf itself does not need to be confidential.

When transferring data to receiving device 300, memory 200 decrypts with a built-in CPU an electronic signature attached to an image by using data authentication algorithm Hcf and nonpublic key Kcf, and returns a correct answer to authentication between SCF and PC mentioned later after ensuring that the image has not been changed since it was recorded. In case change is detected, it returns an error to authentication between SCF and PC.

3. Data transfer from a memory to a receiving device:

Any data recorded in NAND record space 210 of memory 200 is transferred to record space 310 of receiving device 300. On this occasion, device authentication is performed between authentication section 232 of memory 200 and authentication section 320 of receiving device 300, and only if authentication is successful, data transfer is implemented from NAND record space 210 to record space 310. When reading data from memory 200, receiving device 300 performs authentication to authentication section 232 of memory 200 based on mutually common encryption function Hpc and nonpublic key Kpc specified by receiving device 300 so as to verify that it is the normal receiving device 300. In addition, as mentioned above, when transferring data to receiving device 300, memory 200 ensures with a built-in CPU that the image has not been changed since it was recorded by using data authentication algorithm Hcf and nonpublic key Kcf, and then transfers to receiving device 300 the data indicating that it is already ensured. It

is possible to verify that the data is the data which came trough a limited route from predetermined input device 100 based on authentication of memory 200 and information of "confirmation of no change" communicated from memory 200. The following shows a concrete process:

3.1. SPC issues a Send Seed command to CF and informs that a certain random number (= R2) is to be transmitted.

3.2. SPC returns R2 to CF.

3.3. SPC starts reading data. CF usually repeats data transfer of one page (= 512 bytes) 256 times at the maximum per read command.

3.4. SCF first checks by using Hcf and Kcf whether the data to be read by PC is correctly flagged. If not correctly flagged, it determines that the data is not specified and returns an error to authentication for a read command this time.

3.5. If it is correctly flagged, SCF calculates the following expression (2) for the transmitted R2 and returns R_Ep to PC. Kpc is a secret key between SCF and SPC.

$$R_Ep = Hpc(Kpc, R2) \quad (2)$$

3.6. SPC calculates the above expression (2) by using Hpc and Kpc which it has and R2 which was sent to CF, so as to check if the calculated R_Ep matches what came from SCF. If they do not match, it determines that CF or the data to read is not what is specified.

3.7. If a result of calculating R_Ep matches what came from CF, to the read data to be covered, SPC sends a seed and performs authentication at least once each time a read command is sent until all has been read, and only in the case that authentication was correctly performed to all the pages, it determines that the data came from SDC by way

of SCF without being changed. By this series of operations, SPC can verify a source of the received data and whether or not it has been changed. Fig. 2 shows the concept of the above-mentioned authentication and data flow from SDC to SPC via SCF.

Next, a structure of a CompactFlash memory card which is suitably usable in the above-mentioned system for authenticating digital data of the present invention is described. A CompactFlash memory card is a small nonvolatile memory released from SanDisk in 1994, PCMCIA-ATA compatible and electrically and mechanically usable as a PCMCIA card of Type II. It has capacity of 4MB, 8MB, 16MB and so on and has a wide range of uses including storage of a JPEG image (50KB to 100KB) taken by a digital camera. A major characteristic of a CompactFlash memory card is that it has a built-in CPU in spite of its small size and bulk. Fig. 3 shows an example of an internal structure of a CompactFlash memory card, Fig. 4 an example of physical format specifications (8MB) and Fig. 5 an example of a page model. In the present invention, flags are written to a Reserved Area which is a redundant area shown in Fig. 5.

The above concluded description of the main part of a system for authenticating digital data of the present invention. Next, with regard to the other alternatives of operation, examples of operation by a public key, multiplexing of an authentication sector and encryption of Kpc in a PC are described. First,

4. Operation by a public key:

In an authentication facility between SDC and SCF, it is possible to utilize a public key system so as to make it more difficult to write to SCF any image changed by "disguise" of a camera. This can be attained by providing the camera side with a secret key for encrypting data for challenge and the SCF side with a public key for authenticating a reply from the camera.

5. Multiplexing of an authentication sector:

In device authentication, a subject device (SCF in the case of SDC and SCF, SPC in the case of SCF and SPC) sends data for challenge to the other party's device, and concludes it by verifying with cipher on hand the data translated by predetermined encryption and returned. If a device authentication process and following data transfer are separated, there is a danger that "disguise" of a device may occur by switching to a next input device as soon as authentication is completed. To prevent this, it is arranged so that authentication data, mixed with transfer data, is continuously sent from the input device. A rule for mixing authentication data is to generate it from a reply after encrypting challenge data (R_Ed, R_Ep), and the other party's device is authenticated by both direct transfer of authentication data and a rule for transferring that data.

6. An example of encryption of Kpc in a PC:

First, the restrictive conditions in this configuration are as follows.

1. For any attack on contents of a ROM in SDC and SCF, it is taper resist in which a code of a ROM cannot be analyzed from outside and contents of a ROM cannot be analyzed even if it is decomposed. Accordingly, the keys in it (Kdc, Kcf and Kx) cannot be attacked, either.

2. Since Kpc, an encryption key for uploading in SPC is managed by SPC administrator and encrypted, it cannot be estimated by an owner of SCF. In case there is a possibility that an owner of SCF may decrypt an uploaded program of a PC and estimate Kpc in that PC, the following measures may be taken.

   a. When installing Kpc:

      When installing Kpc, a PC administrator calculates Kpc' which is Kpc encrypted by the following expression (3) and stores it in a PC.

      Kpc' = E2pc(password, Kpc) (3)

Here, E2pc is an encryption function for encrypting Kpc, and the password is one that only a PC administrator can know. It also stores in a PC a password' which is the password hashed by the following expression (4). In this case, the password itself is not stored.

Password' = Hpasw(password) (4)

Here, Hpasw is a one-way hash function.

b. When authenticating between SCF and SPC

An SPC administrator enters a password. An uploaded program of SPC calculates expression (4) from the entered password, and if the calculated value matches the stored password', calculates Kpc from the following expression (5) and use it for authentication.

Kpc = D2pc(password, Kpc') (5)

Here, D2pc is a decoding function for E2pc, and the following expression (6) holds for arbitrary values x, y.

x = D2pc(y, E2pc(y, x)) (6)

In this method, even if a malicious person successfully locates Kpc', a password', E2pc, D2pc and Hpasw, it is impossible to estimate Kpc from there.

The above-mentioned advantages of the present invention are summarized as follows.

1. Since device authentication is performed between SDC and SCF and between SCF and

SPC respectively, it is possible to limit a data transfer route from an input device to a receiving device.

2. Data transfer between SDC and SCF and between SCF and SPC are intermittently authenticated by multiplexing an authentication sector to data so as to allow prevention of substitution of an input device without authentication after successful authentication of a device.

3. When recording data in a memory area of SCF, since a signature is implemented by a hash function using a secret key in a ROM of SCF, it can prevent NAND record space 210 from being decomposed and replaced by any changed data.

4. Since authentication keys with SDC and SPC (Kdc and Kpc) are encrypted by a secret key in a ROM (Kx), they cannot be stolen even if NAND record space 210 of SCF is decomposed.

5. Even if device authentication was not performed or failed, data can be recorded in NAND record space 210 and read out in the same manner as an ordinary CF. However, it is not authenticated.

6. Since the system of the present invention can be implemented by modification of a program built into existing hardware, it does not put much of a burden upon a camera manufacturer so that it is expected to spread in the market as a de facto standard.

As it is clear from the above description, the present invention can assure maintenance of data of an input device and a receiving device of digital data in an inexpensive and effective manner so as to allow a digital photograph to become admissible evidence. In addition, since introduction of this technology can be materialized by modification of a program built into existing hardware, it does not put much of a burden upon a camera manufacturer so that it is expected to spread in the market as a de facto standard. It can also promote digitization of companies and

the like which withhold from digitization in terms of safety of transfer data.

What is claimed is:

Sep 15, 2005 15:50:50

CLAIMS

1. A method for authenticating digital data in a system for writing digital data entered from an input device to a memory and transferring the digital data written in the memory to a receiving device, said method comprising the steps of:

when writing digital data from the input device to the memory and transferring the digital data from the memory to the receiving device, authenticating devices between the input device and the memory and between the memory and the receiving device respectively; and

when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, decrypting the implemented electronic signature so as to transfer the digital data after ensuring that it has not been changed since it was recorded.

2. The method of claim 1 comprising the step of:

mixing data for authenticating devices into the digital data to be written from said input device to said memory and the digital data to be transferred from said memory to said receiving device.

3. The method of claim 1 comprising the step of:

implementing by a central processing unit built into said memory authentication between said input device and said receiving device and authentication to the digital data in said memory and decryption of said implemented authentication.

4. The method of claim 1 comprising the step of:

only if authentication between said input device and said memory and between said memory and said receiving device is successful, performing the writing of digital data from said input device to said memory and the transfer of digital data from said memory to said receiving device; and if the authentication is not successful, performing ordinary writing and transfer of digital data.

5. The method of claim 1 wherein:

between said input device and said memory, said system having a specific mutual encryption function Hdc and an internal key Kdc used for authenticating both of them; said memory having a hash function Hcf and an internal key Kcf used for an electronic signature in said memory; and between said memory and said input device, said system having a specific mutual encryption function Hpc and its key Kpc used for authenticating both of them.

6. The method of claim 5 wherein said functions Hdc, Hcf and Hpc and their keys Kdc, and Kcf are stored in a read-only memory of said memory device.

7. The method of claim 6 wherein said key Kpc is encrypted and stored in NAND record space.

8. The method of claim 1 wherein authentication from said input device to said memory is performed by using a public key system.

9. The method of claim 1 wherein said memory is a flash memory and stores said electronic signature on digital data by said hash function into a redundant area not to be calculated by an ECC of each page in an memory area.

SYSTEM FOR AUTHENTICATING DIGITAL DATA

ABSTRACT OF THE DISCLOSURE

A system for authenticating digital data capable of preventing change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data. When writing digital data from an input device to a memory and transferring the digital data from the memory to a receiving device, device authentication is performed between the input device and the memory and between the memory and the receiving device respectively. At the same time, when writing digital data to the memory, in the case of implementing on the digital data an electronic signature by a one-way hash function and also reading from the memory and transferring the digital data, the implemented electronic signature is decrypted so as to transfer the digital data after ensuring that it has not been changed since it was recorded. Thus, it is possible to prevent change or disguise of data by improvement or interchange in case of no confidentiality in the data itself so as to maintain the data.

Copyright - IBM Corp.

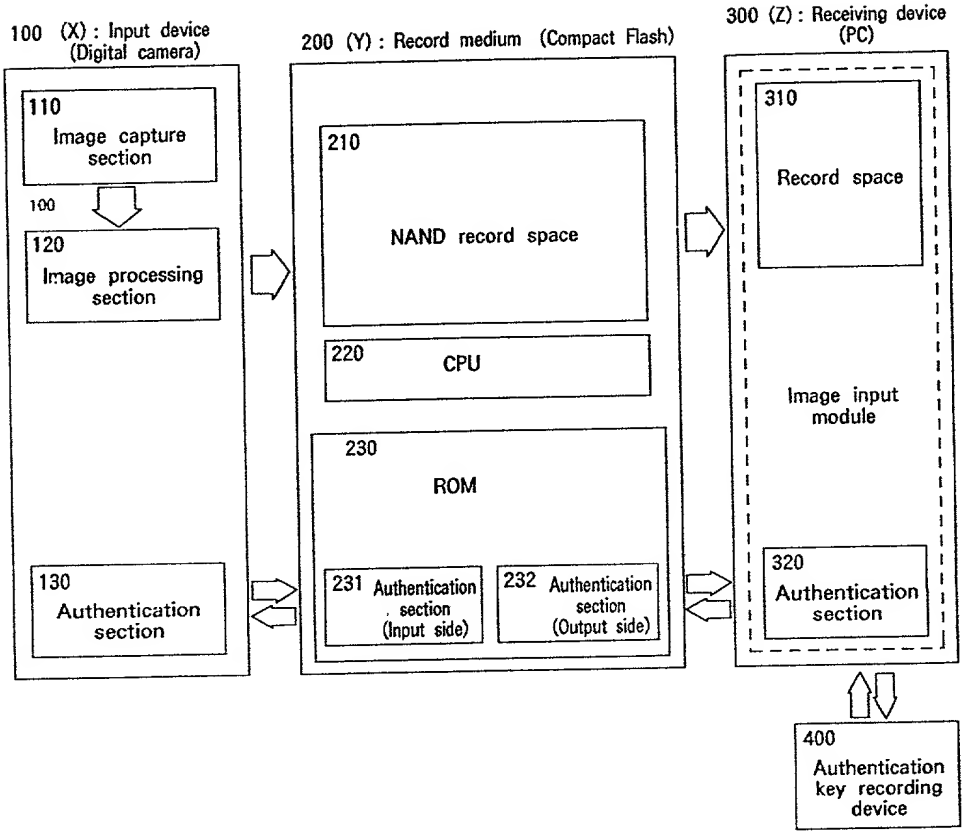
100 (X) : Input device (Digital camera)
110 Image capture section
100
120 Image processing section
130 Authentication section
200 (Y) : Record medium (Compact Flash)
210 NAND record space
220 CPU
230 ROM
231 Authentication section (Input side)
232 Authentication section (Output side)
300 (Z) : Receiving device (PC)
310 Record space
Image input module
320 Authentication section
400 Authentication key recording device

Fig. 1

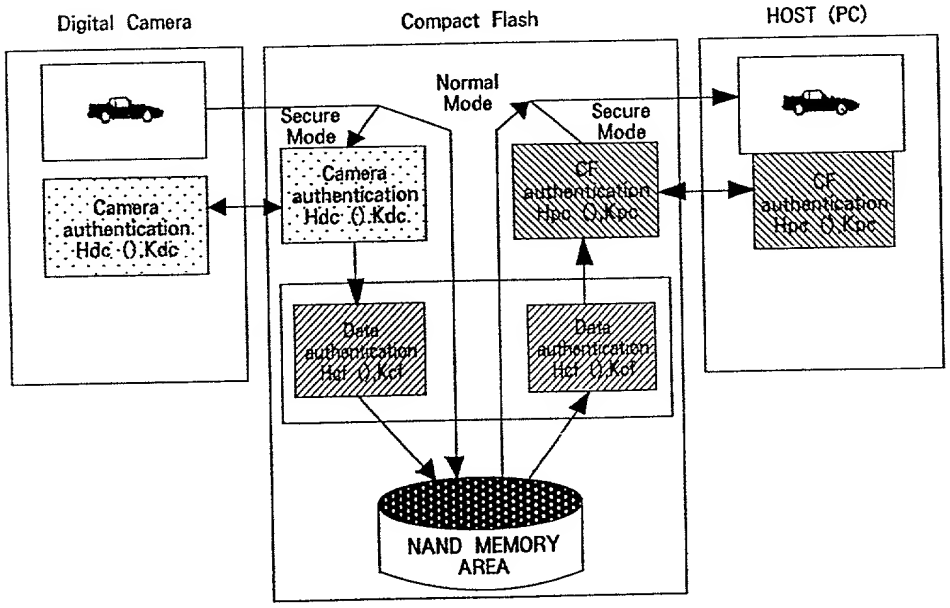
Digital Camera
Compact Flash
HOST (PC)
Normal Mode
Secure Mode
Secure Mode
Camera authentication Hdc () Kdc
Camera authentication Hdc () Kdc
CF authentication Hpc () Kpc
CF authentication Hpc () Kpc
Data authentication Hcf () Kcf
Data authentication Hcf () Kcf
NAND MEMORY AREA

Fig. 2

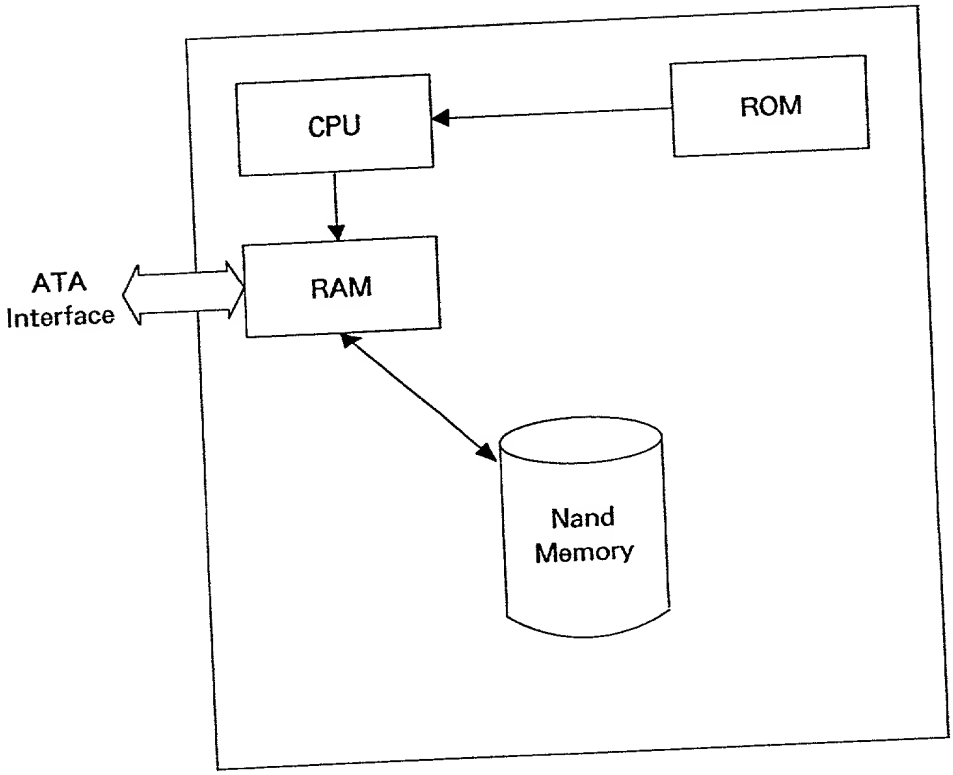

Fig. 3

09/15/2004, EAST Version: 1.4.1

		0 – 511	512 – 527
Block 0	Page 0	Data area (512Byte)	Redundant section (16Byte)
	Page 1		
	:		
	Page 15		
Block 1	Page 0		
	Page 1		
	:		
	Page 15		
:	:	:	:
:	:	:	:
:	:	:	:
:	:	:	:
:	:	:	:
Block 999	Page 0		
	Page 1		
	:		
	Page 15		

Fig. 4

05/05/99, EAST Version: 1.03.0002

◎Data area (512Byte)

Byte	All pages
0 ~ 255	Data Area – 1
256 ~ 511	Data Area – 2

◎Redundant area (16Byte)

Byte	All pages
512	Reserved Area
513	
514	
515	
516	Data Status Area
517	Block Status Area
518	Block Address Area – 1
519	
520	ECC Area – 2
521	
522	
523	Block Address Area – 2
524	
525	ECC Area – 1
526	
527	

Fig. 5

Docket No.
JA9-98-173

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

SYSTEM FOR AUTHENTICATING DIGITAL DATA

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International Application Number _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
JP 10-372355	**Japan**	**28 December 1998**	☐
(Number)	(Country)	(Day/Month/Year Filed)	
			☐
(Number)	(Country)	(Day/Month/Year Filed)	
			☐
(Number)	(Country)	(Day/Month/Year Filed)	

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional

(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)
(Application Serial No.)	(Filing Date)	(Status) (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

William B. Porter, Reg. No. 33,135
Floyd A. Gonzalez, Reg. No. 26,732
Lynn L. Augspurger, Reg. No. 24,227
William A. Kinnaman, Jr., Reg. No. 27,650
Lily Neff, Reg. No. 38,254
Marc A. Ehrlich, Reg. No. 39,966
Lawrence D. Cutter, Reg. No. 28,501
Christopher A. Hughes, Reg. No. 26,914
Edward A. Pennington, Reg. No. 32,588
John E. Hoel, Reg. No. 26,279
Joseph C. Redmond, Reg. No. 18,753

Send Correspondence to: **William A. Kinnaman, Jr.**
IBM Corporation, IPLAW
522 South Road, M/S P386
Poughkeepsie, NY 12601-5400

Direct Telephone Calls to: *(name and telephone number)*
William A. Kinnaman, Jr. **(914) 433-1175**

Full name of sole or first inventor **Koichi Kamijo**
Sole or first inventor's signature Date
Residence **1-18-16-205 Aobadai, Aoba-ku, Yokohama-shi, Kanagawa-ken, Japan**
Citizenship **Japan**
Post Office Address **1-18-16-205 Aobadai, Aoba-ku, Yokohama-shi, Kanagawa-ken, Japan**

Full name of second inventor, if any **Norishige Morimoto**
Second inventor's signature Date
Residence **1-18-11-501 Kinuta, Setagaya-ku, Tokyo-to, Japan**
Citizenship **Japan**
Post Office Address **1-18-11-501 Kinuta, Setagaya-ku, Tokyo-to, Japan**

Full name of third inventor, if any **Akio Koide**
Third inventor's signature Date
Residence **1-3-13-709 Minamiyamada, Tsuzuki-ku, Yokohama-shi, Kanagawa-ken, Japan**
Citizenship **Japan**
Post Office Address **1-3-13-709 Minamiyamada, Tsuzuki-ku, Yokohama-shi, Kanagawa-ken, Japan**

Full name of fourth inventor, if any **Tohru Sakakura**
Fourth inventor's signature Date
Residence **1-4-B-306 Wakakusadai, Aoba-ku, Yokohama-shi, Kanagawa-ken, Japan**
Citizenship **Japan**
Post Office Address **1-4-B-306 Wakakusadai, Aoba-ku, Yokohama-shi, Kanagawa-ken, Japan**

Full name of fifth inventor, if any
Fifth inventor's signature Date
Residence
Citizenship
Post Office Address

Full name of sixth inventor, if any
Sixth inventor's signature Date
Residence
Citizenship
Post Office Address